UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/681,804	06/07/2001	James Terry Dollens		5344

28953 7590 09/14/2004

JAMES TERRY DOLLENS
1675 COX RD
ROSWELL, GA 30075

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	**PAPER NUMBER**
2131	2

DATE MAILED: 09/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/681,804	DOLLENS, JAMES TERRY	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-28 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-28 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-28 are presented for examination.

Specification

Content of Specification

(a) Title of the Invention: See 37 CFR 1.72(a) and MPEP § 606. The title of the invention should be placed at the top of the first page of the specification unless the title is provided in an application data sheet. The title of the invention should be brief but technically accurate and descriptive, preferably from two to seven words may not contain more than 500 characters.

(b) Cross-References to Related Applications: See 37 CFR 1.78 and MPEP § 201.11.

(c) Statement Regarding Federally Sponsored Research and Development: See MPEP § 310.

(d) Incorporation-By-Reference Of Material Submitted On a Compact Disc: The specification is required to include an incorporation-by-reference of electronic documents that are to become part of the permanent United States Patent and Trademark Office records in the file of a patent application. See 37 CFR 1.52(e) and MPEP § 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text were permitted as electronic documents on compact discs beginning on September 8, 2000.

Or alternatively, Reference to a "Microfiche Appendix": See MPEP § 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.

(e) Background of the Invention: See MPEP § 608.01(c). The specification should set forth the Background of the Invention in two parts:

(1) Field of the Invention: A statement of the field of art to which the invention pertains. This statement may include a paraphrasing of the applicable U.S. patent classification definitions of the subject matter of the claimed invention. This item may also be titled "Technical Field."

(2) Description of the Related Art including information disclosed under 37 CFR 1.97 and 37 CFR 1.98: A description of the related art known to the applicant and including, if applicable, references to specific related art and problems involved in the prior art which are solved by the applicant's invention. This item may also be titled "Background Art."

(f) Brief Summary of the Invention: See MPEP § 608.01(d). A brief summary or general statement of the invention as set forth in 37 CFR 1.73. The summary is separate and distinct from the abstract and is directed toward the invention rather than the disclosure as a whole. The summary may point out the advantages of the invention or how it solves problems previously existent in the prior art (and preferably indicated in the Background of the Invention). In chemical cases it should point out in general terms the utility of the invention. If possible, the nature and gist of the invention or the inventive concept should be set forth. Objects of the invention should be treated briefly and only to the extent that they contribute to an understanding of the invention.

(g) Brief Description of the Several Views of the Drawing(s): See MPEP § 608.01(f). A reference to and brief description of the drawing(s) as set forth in 37 CFR 1.74.

(h) Detailed Description of the Invention: See MPEP § 608.01(g). A description of the preferred embodiment(s) of the invention as required in 37 CFR 1.71. The description should be as short and specific as is necessary to describe the invention adequately and accurately. Where elements or groups of elements, compounds, and processes, which are conventional and generally widely known in the field of the invention described and their exact nature or type is not necessary for an understanding and use of the invention by a person skilled in the art, they should not be described in detail. However, where particularly complicated subject matter is involved or where the elements, compounds, or processes may not be commonly or widely known in the field, the specification should refer to another patent or readily available publication which adequately describes the subject matter.

(i) Claim or Claims: See 37 CFR 1.75 and MPEP § 608.01(m). The claim or claims must commence on separate sheet or electronic page (37 CFR 1.52(b)(3)). Where a claim sets forth a plurality of elements or steps, each element or step of the claim should be separated by a line indentation. There may be plural indentations to further segregate subcombinations or related steps. See 37 CFR 1.75 and MPEP § 608.01(i)-(p).

(j) Abstract of the Disclosure: See MPEP § 608.01(f). A brief narrative of the disclosure as a whole in a single paragraph of 150 words or less commencing on a separate sheet following the claims. In an international application which has entered the national stage (37 CFR 1.491(b)), the applicant need not submit an abstract commencing on a separate sheet if an abstract was published with the international application under PCT Article 21. The abstract that appears on the cover page of the pamphlet published by the International Bureau (IB) of the World Intellectual Property Organization (WIPO) is the abstract that will be used by the USPTO. See MPEP § 1893.03(e).

(k) Sequence Listing, See 37 CFR 1.821-1.825 and MPEP §§ 2421-2431. The requirement for a sequence listing applies to all sequences disclosed in a given application, whether the sequences are claimed or not. See MPEP § 2421.02.

2. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

Information Disclosure Statement

3. The listing of references in the specification is not a proper information disclosure statement. 37 CFR 1.98(b) requires a list of all patents, publications, or other information submitted for consideration by the Office, and MPEP § 609 A(1) states, "the list may not be incorporated into the specification but must be submitted in a separate paper." Therefore, unless the references have been cited by the examiner on form PTO-892, they have not been considered.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-28 are rejected as failing to define the invention in the manner required by 35 U.S.C. 112, second paragraph.

6. The claim(s) are narrative in form and replete with indefinite and functional or operational language. The structure which goes to make up the device must be clearly and positively specified. The structure must be organized and correlated in such a manner as to present a complete operative device. The claim(s) must be in one sentence form only. Note the format of the claims in the patent(s) cited.

7. Claim 4 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Applicant refers to a "method 6" in claim 4. Method 6 is not defined in any preceding or following claim or the specification, thereby rendering the claim indefinite.

8. Claim 13 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Applicant refers to "method 12" and "method 10" in claim 13. Methods 12 and 10 are not defined in any preceding or following claim or the specification, thereby rendering the claim indefinite.

9. Claims 14 and 15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Applicant refers to a "method 13" in claim 14. Method 13 is not defined in any preceding or following claim or the specification, thereby rendering the claim indefinite.

10. Claims 17-28 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Applicant refers to a "method 13" in claim 17. Method 13 is not defined in any preceding or following claim or the specification, thereby rendering the claim indefinite.

11. Claim 19 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Applicant refers to a "method 18" in claim 19. Method 13 is not defined in any preceding or following claim or the specification, thereby rendering the claim indefinite.

12. Claims 22-24 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Applicant refers to "method 21" and "method 13" in claim 22. Methods 21 and 13 are not defined in any preceding or following claim or the specification, thereby rendering the claim indefinite.

13. Claims 26-28 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Applicant refers to "method 24" and "method 25" in claim 26. Methods 24 and 25 are not defined in any preceding or following claim or the specification, thereby rendering the claim indefinite.

14. Claim 8 recites the limitation "storing the DNA Pattern in the EDSS." There is insufficient antecedent basis for this limitation in the claim. Emphasis added.

15. Claim 11 recites the limitation "retrieving the DNA Pattern from the EDSS." There is insufficient antecedent basis for this limitation in the claim. Emphasis added.

16. Claim 16 recites the limitation "storing control information into an EDSS file record." There is insufficient antecedent basis for this limitation in the claim. Emphasis added.

17. Claim 19 recites the limitation "searching the EDSS." There is insufficient antecedent basis for this limitation in the claim. Emphasis added.

18. Claim 20 recites the limitation "the object is rejected is the object name is not found on the EDSS." There is insufficient antecedent basis for this limitation in the claim. Emphasis added.

19. Claim 21 recites the limitation "the step of extracting control information from a record corresponding to the DNA Steganographic Object of the EDSS." There is insufficient antecedent basis for this limitation in the claim. Emphasis added.

20. Claim 25 recites the limitation "retrieving the DNA Pattern definition from the EDSS file." There is insufficient antecedent basis for this limitation in the claim. Emphasis added.

21. Where applicant acts as his or her own lexicographer to specifically define a term of a claim contrary to its ordinary meaning, the written description must clearly redefine the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the applicant intended to so redefine that claim term. *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). The term "DNA" in claims 3, 4, 6-13, 15-17, 19, and 21-25 is used by the claim to mean "a unique network configuration signature that details the contents of a network and the computers attached to the aforementioned network", while the accepted meaning is "deoxyribonucleic acid, which is the genetic material necessary for the organization and functioning of most living cells." The term is indefinite because the specification does not clearly redefine the term.

Claim Rejections - 35 USC § 102

22. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

23. Claims 1-14 and 16-28 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,919,257 to Trostle, hereinafter Trostle.

24. As per claim 1, Trostle teaches a method for intrusion detection of a computer system that identifies prior to execution computer system objects that have been changed or new objects added by unauthorized entities said method comprises the phases of:

definition, creation and authentication, see column 2, line 25 to column 3, line 30 and column 4, line 64 to column 5, line 46. Wherein the definition phase is drawn to the user object, which indicates all of the executables located on the client workstation. The creation phase is drawn to the modules created by the server to be executed on the client workstation in order to detect any changes made to the client workstation. The authentication phase is discussed in column 2, lines 25-37 and is performed to detect any unauthorized changes made to the client workstation.

25. Regarding claim 2, Trostle teaches the steps of the intrusion detection environment definition, see column 2, lines 25-33.

26. With regards to claim 3, Trostle teaches wherein the step of defining the DNA Domain, which is the environment where computer system objects reside, and is managed by the DNA Domain Administrator, who is an individual or group responsible for authorizing new objects to enter the DNA Domain, see column 1, line 66 to column 2, line 8 and column 2, line 61 to column 3, line 7. Wherein the DNA domain is drawn to the network in which the client workstation resides and the DNA Domain Administrator is drawn to the system administrator mentioned in the paragraph bridging columns 2 and 3.

27. With regards to claim 4, Trostle teaches wherein the step of defining the DNA Scope Set, which is a set of objects, coined DNA Objects, residing in the DNA Domain having the same DNA Pattern, which is defined in method 6, see column 3, lines 8-17 and column 5, lines 1-26. The DNA Scope Set is drawn to the list of executable programs to be checked, wherein the executable programs drawn to the DNA Objects. In this case, Trostle discloses that the browsers, mail programs, and certain portions of the operating system should consistently be checked. These programs would all have similar identifiers on each individual workstation that would need to be checked in order to detect any unauthorized changes that may have been made.

28. With regards to claim 5, Trostle teaches wherein the step of defining an external data storage structure (EDSS) that is a container for control information for the intrusion detection system, see column 2, lines 3-37, Trostle's discussion of storing the to-be-downloaded modules for the workstation at the server.

29. With regards to claim 6, Trostle teaches wherein the step of defining the DNA Pattern, which is a sequence of identifier fields that will serve to create a unique copy of the object and create an ownership token between the object and the operating system, see column 2, lines 25-37, as well as column 5, lines 2-18.

30. Concerning claim 7, Trostle teaches wherein the DNA Pattern is selected from the properties of the computer system objects (DNA Objects) in the DNA Scope Set such that the

DAN Pattern is unique across the DNA Domain when compared to other DNA Patterns, see column 2, lines 25-37, as well as column 3, lines 7-18 and column 5, lines 2-18.

31. Concerning claim 8, Trostle teaches wherein the step of storing the DNA Pattern in the EDSS, see column 2, lines 3-37, Trostle's discussion of storing the to-be-downloaded modules for the workstation at the server.

32. Regarding claim 9, Trostle teaches the creation phase, which inserts the DNA Pattern into DNA Scope Set objects creating DNA Steganographic Objects, see column 6, lines 53-67.

33. With regards to claim 10, Trostle teaches wherein the step of selecting DNA Objects from the DNA Domain to be protected, see column 3, lines 7-18 and column 6, lines 53-67.

34. With regards to claim 11, Trostle teaches wherein the step of retrieving the DNA Pattern from the EDSS, see column 2, lines 25-37 and column 7, lines 1-10. Wherein the retrieving the DNA pattern is drawn to downloading or receiving the modules from the server.

35. With regards to claim 12, Trostle teaches wherein the step of encrypting the DNA Pattern, see column 5, lines 27-47.

36. With regards to claim 13, Trostle teaches wherein the step of a steganographic process to embed the results of method 12 into the results of method 10 producing a DNA Steganographic Object, see column 3, lines 7-18, column 5, lines 27-47, and column 6, lines 53-67.

37. With regards to claim 14, Trostle teaches wherein comprises the step of storing the results of method 13 in the system resource library, see column 7, lines 32-41.

38. With regards to claim 16, Trostle teaches wherein the step of storing control information into an EDSS file record relative to the DNA Steganographic Object so as to be able to extract the DNA Pattern from the DNA Steganographic Object and recreate the DNA Object, see column 6, lines 52-67.

39. Regarding claim 17, Trostle teaches the steps of the authentication phase, which extracts a DNA Pattern from the DNA Steganographic Object (the results of method 13) recreating the DNA Object, see column 5, line 66 to column 6, line 42.

40. With regards to claim 18, Trostle teaches wherein the step of the operating system providing the intrusion detection system with an object name to be executed, see column 4, lines 51-63 and column 6, lines 42-67.

41. With regards to claim 19, Trostle teaches wherein the step of searching the EDSS for a record containing a DNA Steganographic Object having the same name as the results of method 18, see column 4, lines 51-63.

42. With regards to claim 20, Trostle teaches wherein the object is rejected is the object name is not found on the EDSS, see column 4, line 64 to column 5, line 17.

43. With regards to claim 21, Trostle teaches wherein comprises the step of extracting control information from a record corresponding to the DNA Steganographic Object of the EDSS file, see column 6, lines 52-67.

44. With regards to claim 22, Trostle teaches wherein comprises the step of, given the control information from method 21, reversing the steganographic process of method 13 to extract the encrypted DNA Pattern see column 6, lines 52-67.

45. Concerning claim 23, Trostle teaches the step of recreating the DNA Object, see column 7, lines 1-41.

46. Concerning claim 24, Trostle teaches the step of decrypting the DNA Pattern, see column 7, lines 1-41.

47. With regards to claim 25, Trostle teaches wherein comprises the step of retrieving the DNA Pattern definition from the EDSS file, see column 4, lines 51-64.

48. With regards to claim 26, Trostle teaches wherein comprises the step of comparing the results of method 24 with the results of method 25, see column 6, lines 28-42 and column 7, lines 27-41.

49. Concerning claim 27, Trostle teaches wherein further authenticates the object for execution if there is a match, see column 6, lines 47-53 and column 7, lines 27-41.

50. Concerning claim 28, Trostle teaches wherein rejects the object if there is no match, see column 6, lines 28-42 and column 7, lines 27-41.

Claim Rejections - 35 USC § 103

51. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

52. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Trostle.

53. Concerning claim 15, Trostle does not teach the step of moving the original DNA Object off-line. It would have been obvious to one of ordinary skill in the art at the time the invention was made to move the original DNA object off-line, since you would be removing the element from the network thus making it inaccessible to malicious users. See MPEP § 2144.04; see *In re*

Karlson, 311 F.2d 581, 583, 136 USPQ 184, 186 (CCPA 1963); see *In re Kuhle*, 526 F.2d 553, 188 USPQ 7 (CCPA 1975).

Remarks

54. Should the claim language of claims 4, 13, 14, 17, 19, 22, and 26 recite "the method of claim <number>" instead of "method <number>" the claims will be objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim cannot reference two claims. See MPEP § 608.01(n).

55. If the claim language of claims 4, 13, 14, 17, 19, 22, and 26 is referring to actual methods defined in the specification the Applicant is reminded that although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

56. The Applicant is also reminded that recitations that occur in the preamble are not given patentable weight. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

Conclusion

57. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

58. The following patents are cited to further show the state of the art with respect to intrusion detection systems, such as:

United States Patent No. 6,647,400 to Moran, which is cited to show analyzing file systems to detect intrusions.

United States Patent No. 6,408,391 to Huff et al., which is cited to show dynamic system defense for information warfare.

59. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (703) 305-7704. The examiner can normally be reached on Monday thru Thursday 7-5.

60. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

61. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100